Zranitelnosti webových aplikací 1 - Útoky proti uživatelům

Kód kurzu: GOC541

Toto školení vás zasvětí do tajů webhackingu a zranitelností webových aplikací, které umožňují útočit na koncové uživatele služby. Školení Vám umožní do detailu pochopit a v praxi si vyzkoušet metody, které běžně používají útočníci. Zranitelnosti webových aplikací umožňující útoky na koncové uživatele patří mezi nejčastější typy webových zranitelností a důkladně by s nimi proto měli být seznámeni všichni vývojáři a provozovatelé webových aplikací. Přestože to nemusí být na první pohled zřejmé, mohou mít tyto útoky velice vážné dopady včetně kompletního převzetí kontroly nad cílovým systémem. Seznamte se s těmito zranitelnostmi a otestujte si bezpečnost svých webových aplikací dříve, než to za vás udělá nevítaný vetřelec. Vše, co k tomu budete potřebovat, Vás naučíme na tomto praktickém kurzu.

Pro koho je kurz určen

Kurz je určen vývojářům a provozovatelům webových aplikací, kteří chtějí porozumět postupům útočníků při napadání webových aplikací. Na mnoha praktických ukázkách si vyzkoušíme postupy útočníků, při nichž dochází ke krádeži uživatelských účtů, přístupových údajů a relací. Zneužijeme requesty odesílané uživatelem, nebo ukradneme a zneužijeme každé jejich kliknutí.
Kurz můžeme s klidným svědomím doporučit také běžným uživatelům se základní znalostí tvorby webových stránek, kteří by se rádi dozvěděli o možných útocích, jež jim hrozí při běžném surfování na internetu. Na tomto kurzu se dozvíte mnoho informací jak zlepšit bezpečnostní návyky při procházení webových stránek, abyste omezili možná rizika.
Postupy probírané na tomto kurzu jsou platformě nezávislé. Získané vědomosti uplatníte v praxi bez ohledu na to, v jakémkoliv programovacím jazyce vyvýjíte své aplikace.

Co vás naučíme

Náš jedinečný kurz Zranitelnosti webových aplikací 1 - Útoky proti uživatelům vám umožní do detailu pochopit a hlavně si na praktických příkladech vyzkoušet metody, kterých běžně využívají útočníci. V průběhu kurzu si postupně vysvětlíme vše, co potřebujete znát pro obranu proti těmto útočným technikám.

Požadované vstupní znalosti

Kurzu se může zúčastnit každý, kdo má základní znalosti technologií HTML, CSS a Javascript.

Osnova kurzu

Úvod, nástroje

- HTTP protokol
- Použití nástroje Burp Suite
- Web Parameter Tampering / Hidden Fields

Autentizace, Session Management

- Enumerace uživatelů
- Útoky na autentizaci / Guessing
- Captcha – použití a chyby
- Citlivé údaje v URL
- Session Stealing
- Session Prediction
- Session Fixation
- Session Donation
- Cross-Site Cooking

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

- Cross-Subdomain Cooking
- Session Puzzling
- Insufficient Session Expiration
- Insufficient logout
- Logout action availability

Důvěra v uživatele

- Cross-Site Request Forgery (CSRF)
- CSRF a metody GET / POST
- Možnosti obrany před CSRF
- HTTP verb tampering
- Krademe kliknutí pomocí clickjackingu
- Vyplňujeme a odesíláme formuláře pomocí clickjackingu
- Možnosti obrany před clickjackingem

Skriptování na straně klienta

- Cross-Site Scripting (XSS)
- Perzistentní XSS
- Reflektovaný XSS
- DOM based XSS
- Blind XSS
- Self XSS
- Bypass kódu
- Protokoly javascript, vbsctipt, data
- XSS a nastavení Content-Type
- Cross-Site Flashing
- Použití nástroje BeEF
- Obrana před XSS
- Too long cookie value
- Přznak HttpOnly
- Cross-Site Tracing
- Reflected HTTP Request Header
- Open Redirect
- HTTP Response Splitting (CRLF injection)
- HTTPResponse Smuggling
- File Download via Open redirect
- Content Spoofing
- Cross-Site Messaging

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

Zranitelnosti webových aplikací 1 - Útoky proti uživatelům

Krademe uživatelská data

- Únik dat refererm
- Únik dat při redirektu
- Útoky na CORS
- JavaScript Hijacking
- Problémy callbacků
- WWW-Authenticate attack
- Post &Back Attack
- Cross-site WebSocket hijacking

Podíváme se i na další útoky...

- Útoky na local storage
- Útoky na websockety
- Cache Poisoning
- HTTP Parameter Pollution
- Host Header Injection
- Path Relative StyleSheet Import (PRSSI)
- Zneužití uživatele pro napadení intranetu
- Reflected File Download
- CSV injection
- HTTP Response hlavičky pro bezpečný web

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved